

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

UNITED STATES OF AMERICA	:	
	:	
v.	:	Criminal Indictment No.
	:	
TODD CHRISLEY,	:	1:19-CR-297-ELR-JSA
JULIE CHRISLEY, and	:	
PETER TARANTINO	:	

**MICHAEL TODD CHRISLEY AND JULIE CHRISLEY'S MOTION TO
SUPPRESS EVIDENCE SEIZED PURSUANT TO THE SEARCH
WARRANTS FOR EMAILS AND ELECTRONICALLY STORED
INFORMATION AND MEMORANDUM OF LAW IN SUPPORT**

COME NOW Defendants, Michael Todd Chrisley and Julie Chrisley, by and through their undersigned counsel, and, pursuant to Fed. R. Crim. P. 41(h), file this Motion to Suppress Emails and Electronically Stored Information obtained as the result of two unlawful seizures and searches. In support of this Motion, Defendants respectfully show this Court the following:

I. INTRODUCTION

On or about March 1, 2019, the Government obtained two search warrants for virtually every piece of information contained in an AOL email account of Defendant Michael Todd Chrisley and the Google Gmail email accounts of Michael Todd Chrisley and Julie Chrisley. The warrants were executed and both AOL, Inc.

and Google, Inc. provided the contents of the email accounts to the Government. The seizures pursuant to these two search warrants were revealed to Defendants in conjunction with the discovery provided by the Government on December 20, 2019. The search warrants were fatally overbroad. After extracting potentially privileged attorney-client emails, members of the prosecution team then began reviewing tens of thousands of emails without regard to the Defendants' rights to privacy or the restrictions placed upon the review by the parameters of the search warrants. By not limiting review of the emails produced by AOL, Inc. and Google, Inc. but in fact literally "seizing" all of the emails without regard to whether they were within the limitations placed upon the Government by the subject search warrants, the Government exceeded the scope permitted by the search warrants. Accordingly, Defendants respectfully request that the Court suppress all of the evidence obtained in the searches and reviewed by the Government.

II. STATEMENT OF FACTS

Michael Todd Chrisley and Julie Chrisley are a married couple who the indictment alleges have earned millions of dollars in income from as early as 2008 through 2017. (Doc. 1 at ¶¶ 1-5). The indictment further alleges that the Defendants did not timely submit tax payments with their tax returns filed for the years 2009, 2011 and 2012. Id. at ¶ 12. Nor did they timely file or submit tax payments to the IRS for the 2013, 2014, 2015 or 2016 tax years. Id. at ¶ 14. Additionally, the

indictment alleges that the Defendants engaged in a conspiracy to commit bank fraud (18 U.S.C. § 1349), substantive bank fraud (18 U.S.C. § 1344 and § 2), wire fraud conspiracy (18 U.S.C. § 1349), wire fraud (18 U.S.C. § 1343 and § 2), conspiracy to defraud the United States (18 U.S.C. § 371) and tax evasion (26 U.S.C. § 7201 and 18 U.S.C. § 2). Id. at ¶¶ 15-56.

The AOL and Google Warrants

On or about March 1, 2019, IRS Special Agent Larry K. Arrow presented an Application & Affidavit For Search Warrant to obtain information associated with the email addresses mchrisley1@gmail.com and jchrisley1@gmail.com and an Application & Affidavit For Search Warrant for information associated with the email address mchrisley1@aol.com to United States Magistrate Judge Catherine Salinas. Each application was supported by an identical Affidavit in support of the application for a search warrant. A copy of the Affidavits and Warrants are attached to this Motion as EXHIBIT A and EXHIBIT B. Both search warrants were authorized by Magistrate Judge Salinas on March 1, 2019 and required execution on or before March 14, 2019. Id.

Defense counsel has been informed by Government counsel that both AOL, Inc. and Google, Inc. complied with the search warrants and provided all of the electronically stored information associated with the Chrisley email accounts.

The Arrow affidavits set forth the progress of the Government's investigation into the Defendants' alleged activities of bank fraud, wire fraud and tax evasion. The affidavits and warrants sought "the contents of all emails associated with the accounts, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which email was sent, and the size and length of each email to be produced by Google, Inc. and AOL, Inc." Exhibit A and Exhibit B at Attachment B I. The search warrants then authorize the Government to seize "all information described above in Section 1 that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 26, United States Code, Sections 7201 (Tax Evasion), 7203 (Failure to File Federal Income Tax Returns), and 7206(2) (Preparing, or Causing the Preparation of, False Federal Income Tax Returns) as well as violations of Title 18, United States Code, Sections 371 (Conspiracy), 1001 (False Statements), 1343 (Wire Fraud), 1344 (Bank Fraud) and 1349 (Conspiracy to Commit Wire and/or Bank Fraud) involving Michael Todd Chrisley, Julie Chrisley, Peter Joseph Tarantino, and Mark Braddock occurring from January 1, 2005 until the present...". Exhibits A and B at Attachment B II.

Based on the two search warrants that issued, upon Defendants' information and belief, the Government reviewed the *entire contents* of the AOL and Gmail accounts identified in the warrants.

On December 20, 2019, the Government delivered copies of the electronically stored information (ESI) to Defendants, it considered “seized” from AOL and Google pursuant to the warrants. The Government acknowledged that while 20,638 records fall within the scope of the electronic search warrants, a total of “237,986 non-privileged emails, calendar items, contact forms, and/or ‘loose files’, such as PDF files, Word documents and images not attached to emails,” were subject to the Government’s review. Doc. 34, p. 2. The Government received, and apparently continues to review, thousands of emails and documents produced by AOL and Google it has admitted are outside the scope of the warrants. The Government has also informed defense counsel that it did not use an independent “taint team” to review the ESI materials to eliminate emails and documents whose seizure would not be justified by the subject search warrants before review by members of the prosecution team.¹

III. ARGUMENT

A. The AOL and Google Search Warrants Were Constitutionally Overbroad and All Evidence Obtained Therefrom Should Be Suppressed.

1. Fourth Amendment Requirements

¹ The Government did exclude before its review potentially privileged attorney-client communications and attorney work product using a separate and independent filter team of FBI personnel in Washington, D.C. who manage the FBI’s electronic evidence database. These personnel are not otherwise involved in the pending investigation and are not part of the prosecution team according to the Government. Therefore, the Defendants make no claim that the Government has improperly reviewed privileged information.

The Fourth Amendment provides: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. Amend. IV (emphasis added); see also *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013). The purpose of the Fourth Amendment warrant clause is to ensure that “those searches deemed necessary should be as limited as possible.” *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

“[T]he specific evil” in this case “is the ‘general warrant’ abhorred by the colonists, and the problem is not the intrusion *per se*, but of a general, exploratory rummaging in a person’s belongings.” *Id.*; see also *United States v. Blake*, 868 F.3d 960, 973 (11th Cir. 2017); *Galpin*, 720 F.3d at 446 (“[T]he central concern underlying the Fourth Amendment [is] the concern about giving police officers unbridled discretion to rummage at will among a person’s private effects.”) (citing *Arizona v. Gant*, 556 U.S. 332, 345 (2009)). The Constitution limits law enforcement’s rights to search only “the specific areas and things for which there is probable cause to search,” which requires that “that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging

exploratory searches the Framers intended to prohibit.” *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

The Government’s warrants to perform unrestricted searches of the AOL and Google accounts of the Defendants were overbroad, and insufficiently particularized. Accordingly, the Warrants violated the Fourth Amendment, and the evidence seized pursuant to both warrants should be suppressed.

2. Overbreadth.

“[A] warrant is overbroad if its ‘description of the objects to be seized . . . is broader than can be justified by the probable cause upon which the warrant is based.’” *United States v. Lustyik*, 57 F. Supp. 3d 213, 228 (S.D.N.Y. 2014) (quoting *Galpin*, 720 F.3d at 446). Warrants must “specify the items to be seized by their relation to designated crimes.” *United States v. Wey*, 2017 U.S. Dist. LEXIS 91138 at *60-61 (S.D.N.Y. June 13, 2017) (citing *United States v. Buck*, 813 F.2d 588, 590-92 (2d Cir. 1987) (warrant authorizing seizure of “any papers, things or property of any kind relating to [the] previously described crime” was overbroad)).

A conclusory reference to a broad set of federal statutes does not create a narrowness sufficient to ward off concerns of overbreadth. *United States v. Leary*, 846 F.2d 592, 601 (10th Cir. 1988). Courts have held that “even warrants that identify catchall statutory provisions, like the mail fraud or conspiracy statutes, may fail to comply” with the particularization requirement. *Galpin*, 720 F.3d at 445 n. 5;

see, e.g., *Leary*, 846 F.2d at 594 (warrant authorizing search of export company's business records for violation of the "Arms Export Control Act, 22 U.S.C. § 2778, and the Export Administration Act of 1979, 50 U.S.C. App. § 2410," held overbroad); *Voss v. Bergsgaard*, 774 F.2d 402 (10th Cir.1985) (warrant specifying 18 U.S.C. § 371 held overbroad and warrants invalidated); *United States v. Roche*, 614 F.2d 6, 8 (1st Cir.1980) (a limitation of a search to evidence relating to 18 U.S.C. § 1341, the general mail fraud statute, provides "no limitation at all").

A facially deficient warrant may not be cured by information laid out in the accompanying application. See *Groh v. Ramirez*, 540 U.S. 551, 557 (2004) ("[t]he fact that the application adequately described the things to be seized does not save the warrant from its facial invalidity" because the Fourth Amendment "by its terms requires particularity in the warrant"). Despite the allegations of specific statutory violations set forth in the affidavits, the AOL and Google warrants are facially overbroad.

Here, the affidavits and the ensuing warrants provide almost no limitation. Both the AOL and the Google warrant applications name only various catch-all federal crimes: "Title 26, United States Code, Sections 7201, 7203, 7206(2), and Title 26, Sections 371, 1001, 1343, 1344 and 1349." EXHIBIT B at Attachment B. The seizure of an email account for evidence of mail fraud could, arguably, encompass every single item and piece of electronic information contained in or

related to that account. Based on the crimes stated on the face of the warrants, the agent executing the warrants would not have any basis for eliminating any document found in the AOL or Google email accounts. The warrants are, accordingly, facially overbroad and invalid.

Further, a warrant that identifies “generic” or “catch-all” categories of items subject to seizure without any linkage to the suspected criminal activities may be invalidated for overbreadth. *Wey*, 2017 U.S. Dist. LEXIS 91138 at *72-73 (S.D.N.Y. June 13, 2017). The type of property that is “generally in lawful use in substantial quantities” requires “greater care in its description” in a warrant. *Id.* at *73. Specifically, where warrants authorize “virtually a wholesale search and seizure of the business records of the business”, the warrants are “constitutionally infirm” and must be invalidated. *Klitzman, Klitzman & Gallagher v. Krut*, 744 F.2d 955, 960 (3d Cir. 1984) (invalidating warrants executed on a law firm that “allowed the seizure of all” business records “without regard to whether the materials had any connection to particular alleged crimes”).

Attachment B as to both warrant applications states the documents and information to be seized include “...all information...that constitutes fruits, contraband, evidence, and instrumentalities of violations...”. Exhibit A at Attachment B II. This overbroad catch-all opens the door for the Government to seize nearly all emails of the Defendants.

In theory, the result of the execution of the warrants with this overbroad, catch-all category of documents is that agents, in searching through any communications, representations, or documents of the Defendants could conceivably review and seize any and all emails in the AOL and Google accounts. In practice, that is exactly what happened. Such overbreadth permitted the federal agents and prosecutors to rummage through all of Defendants' day-to-day operations in the possession of AOL and Google. Upon information and belief, the Government reviewed the entirety of the Defendants' three accounts. The "grave dangers inherent in executing a search warrant" for objects whose responsiveness to the warrant is not easily ascertainable means that "responsible officials, including judicial officials, must take care to assure that [such searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy." *Andersen v. Maryland*, 427 U.S. 463, 482 n. 11 (1976).

Although the warrants ostensibly limit the documents to be seized by providing suggested categories of documents and information, the warrants are not truly limited in scope. Instead, the broad categorical language authorized agents to seize nearly all of the Defendants' emails and attachments. The premise that there is a distinction between what is "disclosed" to the Government and what is actually "seized" is a fantasy.

Based on an explanation of how the emails have been reviewed provided by the Government, there is no indication that the Government limited its seizure or review in any respect, including by subject matter, type of activity, date range, or otherwise. The warrants, driven by the Government's over-reaching, became impermissible "general warrants." The remedy is suppression of all fruits of the overbroad and insufficiently particularized warrants.

B. The Government's Execution/Seizure Resulted in the Review of Information Outside of Authority Granted by the Search Warrants.

The manner in which a warrant is executed is subject to later review as to its reasonableness. *Dalia v. United States*, 441 U.S. 238 (1979).

After the production of every electronic document in Defendants' AOL and Google email accounts, the Government apparently took the opportunity to have an unmonitored rummage through the hundreds of thousands of emails seized, without any regard for the restrictions set forth in the Search Warrants. This seizure demonstrates reckless disregard for, if not a blatant violation of, the Fourth Amendment.

At the time of the seizures, there could have been no doubt in the minds of the Government agents that the accounts – unrestricted by search terms or other limiters – would contain documents and information not authorized for seizure or review by the Government.

The Government's blatant intrusion into the Defendants' material it is not authorized to seize is not a hypothetical or abstract concern on the part of the Defendants. Once potentially privileged emails had been filtered out, it is clear that the Government took the opportunity to rummage through every single email, attachment and document whether or not responsive to the parameters set by the issuing Magistrate Judge. The only reasonable conclusion is that the Government acted with open disregard for the Fourth Amendment protection enjoyed by the Defendants.

1. The Seizure Process Violated the Fourth Amendment's Reasonableness Requirement.

“The ultimate touchstone of the Fourth Amendment is ‘reasonableness’.” *Brigham City v. Stuart*, 597 U.S. 398, 403 (2006). It is axiomatic that searches “must be conducted in a reasonable manner, approximately limited to the scope and intensity called for by the warrant.” *United States v. Heldt*, 668 F.2d 1238, 1256 (D.C. Cir. 1991) (citation and footnotes omitted). This governs both Fourth Amendment analysis and acceptable execution of a search warrant. *United States v. Ramirez*, 523 U.S. 65, 71 (1998).

The AOL and Google search warrants produced all emails contained in the Defendants' accounts. The Government's course of conduct in reviewing every single item produced by Google and AOL resulted in the actual seizure and review

of copious amounts of electronically stored information, hard-copy documents and physical items that were beyond the scope of the warrants.

2. A Taint Team Should Have Been Used.

“Because the degree of privacy secured to citizens by the Fourth Amendment has been impacted by the advance of technology, the challenge is to adapt traditional Fourth Amendment concepts to the Government’s modern, more sophisticated investigative tools.” *United States v. Ganias*, 755 F.3d 125, 134 (2nd Cir. 2014).

After the initial production by AOL and Google, the Government should have used a process to identify the data, and seize only, the data within the scope of the warrants. The Government acted unreasonably in reviewing all of the information produced by AOL and Google.

According to the Government, after AOL and Google produced the ESI and potentially privileged emails were filtered out by the independent team, the ESI consisting of 237,986 records, was turned over to the agents and attorneys on the prosecution team who began to read and examine the contents. A “taint team” was not used to further review the seized materials. This process is obviously flawed: the Government’s agents and prosecutors had unfettered access to the entire set of information provided – a cache of data which included information outside the already broad scope of the warrants. This allowed prosecution team members to review information far beyond what was authorized by the warrants. See *United*

States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1179 (9th Cir. 2010) (en banc) (Kozinski, C. J. concurring) (only specially trained computer personnel independent of the investigation should review and segregate nonresponsive data; access by agents involved in investigations should be strictly limited to responsive data) (overruled in part on other grounds, *Demaree v. Pederson*, 887 F.3d 870, 876 (9th Cir. 2018)). Thus, the Government should have employed an independent taint team to conduct the original responsiveness review, but it did not.²

3. The Process Used by the Government to Search the ESI Violated the Two Step Process Authorized by Rule 41(e)(2)(B), Federal Rules of Criminal Procedure.

Rule 41(e)(2)(B) permits an incidental initial overseizure of ESI (Step One) when the entire universe of data is produced to the Government, if the Government then segregates data that is within the scope of the search warrant (Step Two). Here the Government's second search was allowed to ultimately seize and review considerable materials unauthorized by the warrant. As stated above, the Government admits that other than filtering the information provided by AOL and Google for the names and references to attorneys, it conducted no further filter process to eliminate nonresponsive ESI. By failing to engage in the two-step process authorized by Rule 41(e)(2)(B), the Government was permitted to review and obtain

² The Government admits that it searched the entire universe of information provided by AOL and Google. It is unknown whether it used any key words to search for responsive documents.

ESI it was not authorized by the warrants to obtain. See *United States v. Comprehensive Drug Testing, Inc.*, supra, 621 F.3d at 1177 (“the process of segregating electronic data that is seizeable from that that which is not must not become a vehicle for the Government to gain access to data which it has no probable cause to collect”)³.

C. Suppression is Necessary.

While wholesale suppression is an extreme remedy, it is required here. In addition to the facial overbreadth, when a defendant establishes flagrant disregard of the terms of a warrant he or she is entitled to suppression of everything that was seized. To prove flagrant disregard, a defendant must show that “government agents effected a widespread seizure of items that were not within the scope of the warrant and did not act in good faith.” *United States v. Wey*, 256 F.Supp.3d 355, 410 (quoting and citing *United States v. Liu*, 239 F.3d at 140 (internal quotation marks omitted). “[T]o satisfy the first prong...the search conducted by government agents must *actually resemble* a general search.” *Liu*, 239 F.3d at 141 (emphasis in original). “The rationale for blanket suppression is that a search that greatly exceeds the bounds of a warrant and is not conducted in good faith is essentially

³ Defendants acknowledge that existing 11th Circuit case law interpreting Rule 41(e)(2)(B) does not require the use of a taint or filter team.

indistinguishable from a general search.” Id. Accord *United States v. Medlin*, 842 F.2d 1194, 1199 (10th Cir. 1988). Here, suppression is warranted.

The seizure here greatly exceeded the bounds of the warrant and “actually resembled” a general search. The Government was not entitled to seize and review documents for which probable cause was lacking. See *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1172 (9th Cir. 2010) (en banc) (criticizing government “overreach []” in seizure of electronic data unsupported by probable cause). And the harm is clearly irreparable, in that the prosecution team’s review of non-responsive materials cannot be undone. Even without an evidentiary hearing, this motion demonstrates that the government did not act reasonably. By failing to satisfy any two-step process of review for responsiveness by a filter or taint team, it demonstrated “grossly negligent or reckless disregard of the strictures of the Fourth Amendment...precisely the sort of circumstances, rare or not, that call for blanket suppression.” *Wey*, 256 F.3d at 410. By its own admission, the Government claimed access to over 200,000 records when only ten percent (10%) were within the scope of the search warrants authorized by the Court. “Total suppression may be appropriate where the executing officer’s conduct exceeds any reasonable interpretation of the warrant’s provisions.” *United States v. Wuagneux*, 683 F.2d 1343, 1354 (11th Cir. 1982).

D. This Court Should Require the Return of Defendants' Property that is Not Responsive to the Warrants.

Pursuant to Rule 41(g), Federal Rules of Criminal Procedure, Defendants request that this Court return all of the Defendants' seized property (including ESI, hard-copy documents and physical items) that were seized beyond the scope of the search warrants. Of course, Defendants are entitled to the return of all privileged documents that were filtered out prior to the prosecution team's review of the remaining ESI. In addition, the Defendants seek the return of all remaining nonresponsive data. Absent a sufficient justification, the Government should be ordered to return all materials that the search warrants did not authorize it to seize, because it has no legal right to keep them.

WHEREFORE, Defendants respectfully pray for the reasons set forth above, that the Court suppress all evidence and fruits seized pursuant to the warrants at issue in accordance with *Wong Sun v. United States*, 371 U.S. 471 (1963) and the Fourth Amendment to the United States Constitution, and Order the return of the Defendants' property.

Respectfully submitted,

/s/ Bruce H. Morris
Bruce H. Morris
Georgia Bar No. 523575
Counsel for Todd Chrisley

Finestone & Morris, LLP
Suite 2540 Tower Place
3340 Peachtree Road, N.E.
Atlanta, Georgia 30326
(404) 262-2500
bmorris@fmattorneys.com

/s/ Stephen M. Friedberg
Stephen M. Friedberg
Georgia Bar No. 277350
Counsel for Julie Chrisley

Suite 2250, Resurgens Plaza
945 East Paces Ferry Road, NE
Atlanta, Georgia 30326
(404) 842-7243
steve@smflawdawg.com

CERTIFICATE OF SERVICE

I hereby certify that I have this day filed the foregoing “MICHAEL TODD CHRISLEY AND JULIE CHRISLEY’S MOTION TO SUPPRESS EVIDENCE SEIZED PURSUANT TO THE SEARCH WARRANTS FOR EMAILS AND ELECTRONICALLY STORED INFORMATION AND MEMORANDUM OF LAW IN SUPPORT” through this District’s ECF system, which will automatically serve all counsel of record.

This 28th day of February, 2020.

/s/ Bruce H. Morris
Bruce H. Morris